© de Gruyter 2009
J. Math. Crypt. **3** (2009), 1–18 DOI 10.1515 / JMC.2009.xxx

On a conjecture for balanced symmetric Boolean functions

Thomas W. Cusick, Yuan Li and Pantelimon Stănică

Communicated by xxx

Abstract. We give some results towards the conjecture that $X(2^t, 2^{t+1}\ell - 1)$ are the only nonlinear balanced elementary symmetric polynomials over $GF(2)$, where t and ℓ are any positive integers and $X(d,n) = \sum_{1\leq i_1<i_2<\cdots<i_d\leq n} x_{i_1}x_{i_2}\cdots x_{i_d}$.

Keywords. Cryptography, balancedness, symmetry, Boolean functions.

AMS classification. 06E30, 05A10, 11B65, 94C10.

Balancedness is sometimes required for Boolean functions, since we often desire our cryptographic primitives to be unbiased in output. Symmetry is also often required [2, 3], and naturally, one would ask when the two features will intersect. In [5], we conjectured that the polynomials $X(2^t, 2^{t+1}\ell - 1)$ are the *only* nonlinear balanced elementary symmetric polynomials, where $X(d,n) = \sum\limits_{1\leq i_1<\cdots<i_d\leq n} x_{i_1}\cdots x_{i_d}$.

In the present paper we give some results towards this conjecture. In fact, we prove the conjecture for many cases of the parameters involved, but there are some cases still open (which will be mentioned explicitly later in Remark 3.19).

1 Preliminaries

Throughout, $\mathbf{x} = (x_1, \ldots, x_n)$ and $\oplus$ is the addition modulo 2. If f: $GF(2)^n \longrightarrow GF(2)$, then f can be uniquely expressed in the following form, called the *algebraic normal form* (ANF):

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{k_1,k_2,\ldots,k_n\in GF(2)} a_{k_1k_2\ldots k_n} {x_1}^{k_1}{x_2}^{k_2}\cdots {x_n}^{k_n},$$

where each coefficient $a_{k_1k_2\ldots k_n}$ is a constant in $GF(2)$.

The function $f(\mathbf{x})$ is called an *affine function* if $f(\mathbf{x}) = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus a_0$. If $a_0 = 0$, $f(\mathbf{x})$ is also called a *linear function*. We will denote by F_n the set of all functions of n variables and by L_n the set of affine ones. We will call a function *nonlinear* if it is not in L_n. Let $wt(\mathbf{a})$ denote the Hamming weight of a vector $\mathbf{a}$ with entries 0 or 1. The function $f(\mathbf{x})$ is called *symmetric* if any permutation of the x_i leaves the value of the function unchanged.

Research of the third author was partially supported by the Naval Postgraduate School RIP funding.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE
On a conjecture for balanced symmetric Boolean functions

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School,Department of Applied Mathematics,Monterey,CA,93943

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
We give some results towards the conjecture that X(2t; 2t+1‘ &#56256;&#56320; 1) are the only nonlinear balanced elementary symmetric polynomials over GF(2), where t and ‘ are any positive integers and X(d; n) = P 1 i1<i2<   <id n xi1xi2   xid .

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**18**	

2 The balancedness of elementary symmetric polynomials over $GF(2)$

Definition 2.1. For integers n and d, $1 \leq d \leq n$ we define the elementary symmetric polynomial by

$$X(d,n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_d \leq n} x_{i_1} x_{i_2} \cdots x_{i_d}. \tag{2.1}$$

We summarize here some of the results proven in [5]. We let $C(n,k)$ denote the binomial coefficient (recall that if $n < k$, then $C(n,k) = 0$).

Theorem 2.2. *The elementary symmetric polynomial $X(d,n)$ is balanced if and only if $\sum_{0 \leq j \leq n} C(n,j)(-1)^{C(j,d)} = 0$. If $X(d,n)$ is balanced, then $d \leq \lceil n/2 \rceil$. Furthermore, if t, ℓ are positive integers, then $X(2^t, 2^{t+1}\ell - 1)$ is balanced.*

We conjectured [5] that the functions in Theorem 2.2 are the only balanced ones.
Conjecture 1. *There are no nonlinear balanced elementary symmetric polynomials except for $X(2^t, 2^{t+1}\ell - 1)$, where t and ℓ are any positive integers.*

3 The Results

The remainder of the paper will be devoted to the study of Conjecture 1 and proving it for various values of the parameters t, ℓ. A Boolean function $f(\mathbf{x})$ in n variables is said to satisfy the *Strict Avalanche Criterion* ("is SAC" for short) if changing any one of the n bits in the input $\mathbf{x}$ results in the output of the function being changed for exactly half of the 2^n vectors $\mathbf{x}$ with the changed input bit. The SAC concept is relevant for our work because of

Lemma 3.1. *The function $f(\mathbf{x}) = X(d,n)$ is SAC if and only if $X(d-1, n-1)$ is balanced.*

Proof. By definition, f is SAC if and only if $f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a})$ is balanced for all $\mathbf{a} \in GF(2)^n$, with $wt(\mathbf{a}) = 1$. We have $f(\mathbf{x}) \oplus f(\mathbf{x} \oplus (0, \ldots, 0, 1)) = X(d-1, n-1)$, so the lemma is proved. □

By definition any symmetric function is completely determined by the weight of its input, so we can define $v_f(i)$ for $0 \leq i \leq n$ by $f(\mathbf{x}) = v_f(wt(\mathbf{x}))$. Moreover, recall the usual algebraic normal form (ANF) of a Boolean function f in n variables

$$f(x_1, \ldots, x_n) = \bigoplus_{i=0}^{n} \lambda_f(i) \bigoplus_{\mathbf{u}, wt(\mathbf{u}) = i} \prod_{j=1}^{n} x_j^{u_j},$$

where $v_f(i) = \bigoplus_{j \preceq i} \lambda_f(j)$, and $\lambda_f(i) = \bigoplus_{j \preceq i} v_f(j)$, over $GF(2)$ ($j \preceq i$ means that the binary expansion of j is less than the binary expansion of i, in lexicographical order) (see [3, Propositions 1 and 2, p. 2792]).

The ANF of a symmetric function becomes

$$f(x_1, \ldots, x_n) = \bigoplus_{d=0}^{n} \lambda_f(d) X(d, n), \tag{3.1}$$

in our notations. Further, when f is an elementary symmetric function, then $\lambda_f(d) = 1$ is the only nonzero coefficient in the representation (3.1). Moreover,

$$v_f(i) = \bigoplus_{j \preceq i} \lambda_f(j) = \begin{cases} \lambda_f(d), \ if \ d \preceq i \\ 0, \ otherwise. \end{cases} \tag{3.2}$$

We need the following further lemmas. We define the well known Walsh transform $W_f(\mathbf{w})$ by

$$W_f(\mathbf{w}) = \sum_{\mathbf{x} \in GF(2)^n} (-1)^{f(\mathbf{x}) + \mathbf{x} \cdot \mathbf{w}}.$$

Lemma 3.2. *A Boolean function f in n variables is SAC if and only if for every vector $\mathbf{u}$ with $wt(\mathbf{u}) = 1$ and every vector $\mathbf{v}$, we have*

$$\sum_{\mathbf{w} \preceq \bar{\mathbf{u}}} W_f(\mathbf{w} \oplus \mathbf{v})^2 = 2^{wt(\bar{\mathbf{u}}) + n}.$$

Proof. This is a special case of Proposition 1 of Carlet [4, p. 35]. □

Lemma 3.3. *If $f(\mathbf{x})$ in n variables is SAC, then*

$$\sum_{\mathbf{w}: w_n = 0} W_f(\mathbf{w})^2 = \sum_{\mathbf{w}: w_n = 1} W_f(\mathbf{w})^2 = 2^{2n-1}. \tag{3.3}$$

Proof. We use Lemma 3.2 with $\mathbf{v} = \mathbf{0}$ and $\mathbf{u} = (0, \ldots, 0, 1)$. It follows that $wt(\bar{\mathbf{u}}) = n - 1$, so the first sum in (3.3) equals 2^{2n-1}. The two sums add up to 2^{2n} by Parseval's Theorem, so the second sum is also 2^{2n-1}. □

Lemma 3.4. *If $f(\mathbf{x}) = X(d, n)$ is SAC and d is odd, then*

$$W_f(\mathbf{0}) = 2^n - 2\,wt(f) \ \text{ and } W_f(\mathbf{1}) = 2\,wt(f). \tag{3.4}$$

Proof. The first equation in (3.4) is clear for any f, whether or not d is odd.

For the second equation, we observe that by (3.2) our hypotheses imply that $v_f(k) = 0$ for all even k. Since

$$W_f(\mathbf{0}) = \sum_{k=0}^{n} (-1)^{v_f(k)} C(n, k) \text{ and}$$

$$W_f(\mathbf{1}) = \sum_{k=0}^{n} (-1)^{v_f(k) + k} C(n, k),$$

a computation gives

$$W_f(\mathbf{0}) + W_f(\mathbf{1}) = 2^n.$$

Now the second equation in (3.4) follows from the first one. □

We define

$$\begin{aligned} &A = 0,0,1,1;\ \bar{A} = 1,1,0,0;\ B = 0,1,0,1; \bar{B} = 1,0,1,0;\\ &C = 0,1,1,0;\ \bar{C} = 1,0,0,1;\ D = 0,0,0,0; \bar{D} = 1,1,1,1. \end{aligned} \tag{3.5}$$

The next two lemmas are used in the proof of our Theorem 3.8.

Lemma 3.5. (Folklore Lemma [1, Lemma 3.7.2]) *Any affine function f on n variables, $n \geq 2$, is a linear string of length 2^n made up of 4-bit blocks $I_1, \ldots, I_{2^{n-2}}$ given as follows:*

1. *The first block I_1 is one of $A, B, C, D, \bar{A}, \bar{B}, \bar{C}$ or $\bar{D}$.*
2. *The second block I_2 is I_1 or $\bar{I}_1$.*
3. *The next two blocks I_3, I_4 are I_1, I_2 or $\bar{I}_1$, $\bar{I}_2$.*

   ....

$n-1$. *The 2^{n-3} blocks $I_{2^{n-3}+1}, \ldots, I_{2^{n-2}}$ are $I_1, \ldots, I_{2^{n-3}}$ or $\bar{I}_1, ..., \bar{I}_{2^{n-3}}$.*

Lemma 3.6. *We have* $\displaystyle\sum_{\mathbf{x}, wt(\mathbf{x})\ even} (-1)^{\mathbf{x}\cdot\mathbf{w}} = 0$ *for all* $\mathbf{w} \neq \mathbf{0}$ *or* $\mathbf{1}$.

Proof. Let $E(\mathbf{w})$ denote the 2^{n-1}-vector of bits $\mathbf{x}\cdot\mathbf{w} \pmod 2$, where $\mathbf{x}$ runs through the n-vectors $\mathbf{x}$ of even weight in lexicographical order. Thus $E(\mathbf{w})$ lists the exponents in the sum in the lemma. Consider the 2^{n-1} by n array of the vectors $\mathbf{x}$ with even weight, taken in lexicographical order. By the Folklore Lemma, each column in this array is a 2^{n-1}-vector which gives the truth table of a nonconstant linear function in $n-1$ variables. In fact, taking the columns left to right, the functions are simply $x_1, x_2, \ldots, x_{n-1}$, $x_1 \oplus x_2 \oplus \cdots \oplus x_{n-1}$. The vector sum of any subset of at least one and at most $n-1$ of the n columns (corresponding to $\mathbf{w} \neq \mathbf{0}$ or $\mathbf{1}$) is thus the truth table of a nonconstant linear function and so it is balanced. Each vector $E(\mathbf{w})$ is one of these vector sums, so the sum in the lemma is 0. □

Remark 3.7. The sum in Lemma 3.6 is the sum of the Krawtchouk polynomials [9, pp. 130 and 150–153] (variable $y = wt(\mathbf{w})$)

$$P_k(y,n) = \sum_{\mathbf{x}, \mathbf{wt}(\mathbf{x})=\mathbf{k}} (-1)^{\mathbf{x}\cdot\mathbf{w}} = \sum_{j=0}^{k} (-1)^j C(y,j) C(n-y, k-j)$$

of even degree k in y.

Theorem 3.8. *If $f(\mathbf{x}) = X(d,n)$ has odd degree d, then $W_f(\mathbf{w}) = -W_f(\bar{\mathbf{w}})$ for all $\mathbf{w} \neq \mathbf{0}$ or $\mathbf{1}$.*

Proof. Let f be an elementary symmetric function of degree d, that is $f = X(d,n)$. We compute the Walsh transform

$$\begin{aligned} W_f(\overline{\mathbf{w}}) &= \sum_{\mathbf{x}\in GF(2)^n} (-1)^{f(\mathbf{x})+\mathbf{x}\cdot\overline{\mathbf{w}}} = \sum_{\mathbf{x}\in GF(2)^n} (-1)^{f(\mathbf{x})+\mathbf{x}\cdot(\mathbf{1}+\mathbf{w})} \\ &= \sum_{\mathbf{x}\in GF(2)^n} (-1)^{f(\mathbf{x})+wt(\mathbf{x})+\mathbf{x}\cdot\mathbf{w}} = \sum_{k=0}^{n} \sum_{\mathbf{x},wt(\mathbf{x})=k} (-1)^{f(\mathbf{x})+wt(\mathbf{x})+\mathbf{x}\cdot\mathbf{w}} \\ &= \sum_{k=0}^{n} (-1)^{v_f(k)+k} \sum_{\mathbf{x},wt(\mathbf{x})=k} (-1)^{\mathbf{x}\cdot\mathbf{w}}. \end{aligned} \tag{3.6}$$

Next, we use (3.2). Since d is odd, then any integer i with $d \preceq i$ has to be odd, as well. It follows that $v_f(k) = 0$, for any even integer k. Thus, (3.6) becomes

$$\begin{aligned} W_f(\overline{\mathbf{w}}) &= \sum_{k=0}^{n} (-1)^{v_f(k)+k} \sum_{\mathbf{x},wt(\mathbf{x})=k} (-1)^{\mathbf{x}\cdot\mathbf{w}} \\ &= \sum_{k=0,\ even}^{n} (-1)^{v_f(k)} \sum_{\mathbf{x},wt(\mathbf{x})=k} (-1)^{\mathbf{x}\cdot\mathbf{w}} - \sum_{k=0,\ odd}^{n} (-1)^{v_f(k)} \sum_{\mathbf{x},wt(\mathbf{x})=k} (-1)^{\mathbf{x}\cdot\mathbf{w}} \\ &= \sum_{\mathbf{x},\ wt(\mathbf{x})=even} (-1)^{\mathbf{x}\cdot\mathbf{w}} - \sum_{k=0,\ odd}^{n} (-1)^{v_f(k)} \sum_{\mathbf{x},\ wt(\mathbf{x})=k} (-1)^{\mathbf{x}\cdot\mathbf{w}}. \end{aligned}$$

Since

$$\begin{aligned} W_f(\mathbf{w}) &= \sum_{k=0,\ even}^{n} (-1)^{v_f(k)} \sum_{\mathbf{x},wt(\mathbf{x})=k} (-1)^{\mathbf{x}\cdot\mathbf{w}} + \sum_{k=0,\ odd}^{n} (-1)^{v_f(k)} \sum_{\mathbf{x},wt(\mathbf{x})=k} (-1)^{\mathbf{x}\cdot\mathbf{w}} \\ &= \sum_{\mathbf{x},\ wt(\mathbf{x})=even} (-1)^{\mathbf{x}\cdot\mathbf{w}} + \sum_{k=0,\ odd}^{n} (-1)^{v_f(k)} \sum_{\mathbf{x},\ wt(\mathbf{x})=k} (-1)^{\mathbf{x}\cdot\mathbf{w}}, \end{aligned}$$

to prove Theorem 3.8 it will suffice to show that

$$\sum_{\mathbf{x},wt(\mathbf{x})=even} (-1)^{\mathbf{x}\cdot\mathbf{w}} = 0,$$

as long as $\mathbf{w} \neq \mathbf{0}, \mathbf{1}$, and that follows from Lemma 3.6. □

Theorem 3.9. *If $f(x) = X(d,n)$ is SAC and d is odd, then $W_f(\mathbf{0}) = W_f(\mathbf{1})$.*

Proof. By Theorem 3.8, all of the terms except $W_f(\mathbf{0})^2$ and $W_f(\mathbf{1})^2$ in the two sums in (3.3) cancel out (for all other $\mathbf{w}$, $W_f(\mathbf{w})$ is in one sum and $W_f(\bar{\mathbf{w}})$ is in the other sum). By Lemma 3.4, both square roots are positive and we get Theorem 3.9. □

Corollary 3.10. *If d is odd and $f(\mathbf{x}) = X(d,n)$ is SAC, then $wt(f) = 2^{n-2}$.*

Now we determine when $X(d,n)$ is SAC. To deal with the case when d is an even integer, by Lemma 3.1, it is enough to show:

Lemma 3.11. *If $d > 1$ is odd, then $X(d, n)$ is not balanced.*

Proof. Formula (3.2) shows that when $f = X(d, n)$ we have $v_f(i) = 1$ if and only if $d \preceq i$. Thus we have

$$wt(X(d,n)) = \sum_{d \preceq i, i \leq n} C(n,i) \leq \sum_{i\, odd} C(n,i) = 2^{n-1}, \tag{3.7}$$

where the inequality holds because $d \preceq i$ and d odd implies i is odd. If $d > 1$, then $d \preceq i$ cannot hold for all odd $i \leq n$ (in particular, $d \not\preceq d-2$), so the inequality in (3.7) is strict. Therefore, $X(d, n)$ is not balanced. □

Lemma 3.12. *Suppose $d > 1$ is odd. If*

$$d = 2^t + 1 \text{ and } n = 2^{t+1}\ell \text{ for integers } t > 0, \ell > 0, \tag{3.8}$$

then $wt(X(d, n)) = 2^{n-2}$.

Proof. First we observe

$$wt(X(d,n)) = \sum_{d \preceq i, i \leq n} C(n,i) \tag{3.9}$$

because of (3.2), which shows that when $f = X(d, n)$ we have $v_f(i) = 1$ if and only if $d \preceq i$. By (3.9), we need to show that

$$wt(X(d,n)) = \sum_{d \preceq i,\, i \leq n} C(n,i) = 2^{n-2} \tag{3.10}$$

if and only if (3.8) holds. If (3.8) holds, the sum in (3.10) is

$$\begin{aligned} &\sum_{2^t+1 \preceq i,\, i \leq 2^{t+1}\ell} C(2^{t+1}\ell, i) \\ &= \sum_{2^t+1 \preceq i,\, i \leq 2^{t+1}\ell} \Big(C(2^{t+1}\ell - 1, i) + C(2^{t+1}\ell - 1, i-1) \Big) \\ &= \sum_{2^t \preceq i-1,\, i-1 \leq 2^{t+1}\ell - 1} \Big(C(2^{t+1}\ell - 1, i) + C(2^{t+1}\ell - 1, i-1) \Big) \\ &= \sum_{2^t \preceq j,\, j \leq 2^{t+1}\ell - 1} C(2^{t+1}\ell - 1, j) = 2^{n-2}, \end{aligned}$$

(note i is never even in the first three sums, since then $2^t + 1 \preceq i$ is false; this justifies the second last equality, since in the last sum j runs through disjoint pairs of consecutive integers) where the last sum is $wt(X(2^t, 2^{t+1}\ell - 1)$ by (3.9) and so is 2^{n-2} by Theorem 2.2. Thus we have proved that (3.8) implies (3.10). □

We would like to prove the converse of the previous lemma. The following work moves toward that goal, but does not achieve it. Next, we prove five lemmas, which establish many cases of the converse of Lemma 3.12.

Lemma 3.13. *Let $n = 2^{t+1}\ell$ for some strictly positive integers t, ℓ. If j is odd and $2^t + 1 < j < 2^{t+1} + 1$, then $wt(X(j,n)) < 2^{n-2}$.*

Proof. The argument of the previous lemma shows that if (3.8) and (3.10) hold for some given t and ℓ, then the set

$$S(t,\ell) = \{i : 2^t + 1 \preceq i,\, i \le 2^{t+1}\ell = n\}$$

gives a set of binomial coefficients $\{C(n,i) : i \in S(t,\ell)\}$ whose sum is 2^{n-2}. (It is easy to see that $S(t,\ell)$ has $n/4$ elements, but we do not need this fact.) Now suppose that (3.10) holds for $n = 2^{t+1}\ell$ and for some odd $d = j$, say, satisfying $2^t + 1 < j < 2^{t+1} + 1$. Then $wt(j) > 2$, so the set

$$T(j,n) = \{i : j \preceq i,\, i \le 2^{t+1}\ell = n\}$$

is a proper subset of $S(t,\ell)$. Therefore the sum of the binomial coefficients in $\{C(n,i) : i \in T(j,n)\}$ is $< 2^{n-2}$, contradicting our assumption that (3.10) holds with $d = j$. □

Since we refer to it often, we include here for completeness an equation given by Canteaut and Videau in [3] (these sums are called *lacunary sums of binomial coefficients*, see [8]). Results like this concerning the binomial coefficients are very old. Some proofs and references are given in [7].

Lemma 3.14. *For positive integers i, n, p, we have*

$$\begin{aligned} A_n^{2^p}(i) &= \sum_{\substack{0\le j\le n \\ j\equiv i \pmod{2^p}}} C(n,j) \\ &= 2^{n-p} + 2^{1-p}\sum_{j=1}^{2^{p-1}-1}\left(2\cos\left(\frac{j\pi}{2^p}\right)\right)^n \cos\left(\frac{j(n-2i)\pi}{2^p}\right) \end{aligned} \tag{3.11}$$

Lemma 3.15. *Let t, r be positive integers. Suppose that $a_1 > a_3 \ge a_5 \ge \cdots \ge a_J$, with $J = 2K + 1$, are nonnegative integers. Define the sum*

$$\mathbf{T} = \sum_{1\le j\le J} a_j \sin\left(\frac{jr\pi}{2^{t+1}}\right).$$

If $\mathbf{T} = 0$, then $r \equiv 0 \pmod{2^{t+1}}$.

Proof. Write $b_k = a_j$, for $j = 2k + 1$. For convenience, let $\alpha = \frac{r\pi}{2^{t+1}}$. Then, using Abel's summation formula, $\mathbf{T}$ becomes

$$\begin{aligned} \mathbf{T} &= \sum_{k=0}^{K} b_k \sin((2k+1)\alpha) \\ &= \sum_{m=0}^{K-1}(b_m - b_{m+1})\sum_{k=0}^{m}\sin((2k+1)\alpha) + b_K\sum_{k=0}^{K}\sin((2k+1)\alpha). \end{aligned}$$

Note that for the first term where $m = 0$, we have $(b_0 - b_1)\sin\alpha \neq 0$, if $r \neq 0 \pmod{2^{t+1}}$. Also, $(b_m - b_{m+1}) \geq 0$, and $b_K \geq 0$. The conclusion follows once we show that

$$\sin\alpha \quad \text{and} \quad \sum_{k=0}^{m} \sin((2k+1)\alpha)$$

have the same sign. Indeed

$$\begin{aligned}
\sin\alpha \sum_{k=0}^{m} \sin((2k+1)\alpha) &= \frac{1}{2}\sum_{k=0}^{m}(\cos(2k\alpha) - \cos((2k+2)\alpha) \\
&= \frac{1}{2}(1 - \cos((2m+2)\alpha) \geq 0.
\end{aligned}$$

The lemma is proved. □

Remark 3.16. Note that $\mathbf{T}$ above has the same sign as $\sin\alpha$.

Because of Theorem 2.2, there is no loss of generality in taking $n \geq 2(d-1)$ in our next lemma.

Lemma 3.17. *Let r, t be positive integers, $d = 2^t + 1$, $n = 2^{t+1}$, and $r \not\equiv 0 \pmod{2^{t+1}}$. Then $wt(X(d, n+r)) \neq 2^{n+r-2}$.*

Proof. Let $d := 1 + 2^t$ be fixed. Now, using Pascal's identity, we get that $S := wt(X(d, n+r))$ satisfies

$$\begin{aligned}
S &= \sum_{d \preceq i \leq n+r} C(n+r, i) = \sum_{d \preceq i \leq n+r} (C(n+r-1, i) + C(n+r-1, i-1)) \\
&= \sum_{d \preceq i \leq n+r-1} C(n+r-1, i) + \sum_{\substack{2^t \preceq j \leq n+r-1 \\ j\ even}} C(n+r-1, j) \\
&= \sum_{d \preceq i \leq n+r-2} C(n+r-2, i) + \sum_{\substack{2^t \preceq j \leq n+r-1 \\ j\ even}} (C(n+r-1, j) + C(n+r-2, j)) .
\end{aligned}$$

Continuing in this manner, we obtain

$$\begin{aligned}
S &= \sum_{d \preceq i \leq n+r-r} C(2^{t+1}, i) + \sum_{\substack{2^t \preceq j \leq n+r-1 \\ j\ even}} \sum_{k=1}^{r} C(n+r-k, j) \\
&= 2^{n-2} + \sum_{\substack{2^t \preceq j \leq n+r-1 \\ j\ even}} \sum_{k=1}^{r} C(n+r-k, j) \\
&= 2^{n-2} + \sum_{k=1}^{r} \sum_{\substack{2^t \preceq j \leq n+r-1 \\ j\ even}} C(n+r-k, j) \\
&= 2^{n-2} + \sum_{k=1}^{r} \sum_{s=0}^{2^{t-1}-1} \sum_{\substack{j \equiv 2s+2^t \pmod{2^{t+1}} \\ 0 \leq j \leq n+r-1}} C(n+r-k, j).
\end{aligned}$$

We push further the previous identity, by computing the innermost sum. So,

$$\sum_{\substack{j \equiv 2s+2^t \pmod{2^{t+1}} \\ 0 \leq j \leq n+r-1}} C(n+r-k, j) = A_N^{2^{t+1}}(2s+2^t)$$

in the notations of Lemma 3.14, where $N := n+r-k$. Thus, using equation (3.11), we obtain

$$A_N^{2^{t+1}}(2s+2^t) = 2^{n+r-k-t-1} + 2^{-t} \sum_{a=1}^{2^t-1} \left(2\cos\frac{a\pi}{2^{t+1}}\right)^N \cos\frac{a(N-4s-2^{t+1})\pi}{2^{t+1}}.$$

Since

$$\cos\frac{a(N-4s-2^{t+1})\pi}{2^{t+1}} = (-1)^a \cos\frac{a(N-4s)\pi}{2^{t+1}},$$

we get

$$A_N^{2^{t+1}}(2s+2^t) = 2^{n+r-k-t-1} + 2^{-t} \sum_{a=1}^{2^t-1} (-1)^a \left(2\cos\frac{a\pi}{2^{t+1}}\right)^N \cos\frac{a(N-4s)\pi}{2^{t+1}}$$

We obtain

$$\begin{aligned}
S &= 2^{n-2} + \sum_{k=1}^{r} \sum_{s=0}^{2^{t-1}-1} A_N^{2^{t+1}}(2s+2^t) \\
&= 2^{n-2} + \sum_{k=1}^{r} \sum_{s=0}^{2^{t-1}-1} 2^{n+r-k-t-1} \\
&\qquad\qquad + 2^{-t} \sum_{k=1}^{r} \sum_{s=0}^{2^{t-1}-1} \sum_{a=1}^{2^t-1} (-1)^a \left(2\cos\frac{a\pi}{2^{t+1}}\right)^N \cos\frac{a(N-4s)\pi}{2^{t+1}} \\
&= 2^{n-2} + 2^{n+r-2}\sum_{k=1}^{r} 2^{-k} + 2^{-t} \sum_{k=1}^{r} \sum_{s=0}^{2^{t-1}-1} \sum_{a=1}^{2^t-1} (-1)^a \left(2\cos\frac{a\pi}{2^{t+1}}\right)^N \cos\frac{a(N-4s)\pi}{2^{t+1}} \\
&= 2^{n+r-2} + 2^{-t} \sum_{k=1}^{r} \sum_{s=0}^{2^{t-1}-1} \sum_{a=1}^{2^t-1} (-1)^a \left(2\cos\frac{a\pi}{2^{t+1}}\right)^N \cos\frac{a(N-4s)\pi}{2^{t+1}}.
\end{aligned}$$

Therefore, to prove our assertion, we need to show that

$$\begin{aligned}
T: &= \sum_{k=1}^{r} \sum_{s=0}^{2^{t-1}-1} \sum_{a=1}^{2^t-1} (-1)^a \left(2\cos\frac{a\pi}{2^{t+1}}\right)^{n+r-k} \cdot \cos\frac{a(n+r-k-4s)\pi}{2^{t+1}} \\
&= \sum_{k=1}^{r} \sum_{a=1}^{2^t-1} (-1)^a \left(2\cos\frac{a\pi}{2^{t+1}}\right)^{n+r-k} \cdot \sum_{s=0}^{2^{t-1}-1} \cos\frac{a(n+r-k-4s)\pi}{2^{t+1}} \neq 0.
\end{aligned}$$

Since

$$\frac{a(n+r-k-4s)\pi}{2^{t+1}} = a\pi + \frac{(r-k-4s)a\pi}{2^{t+1}},$$

and so,

$$\cos\left(\frac{a(n+r-k-4s)\pi}{2^{t+1}}\right) = (-1)^a \cos\left(\frac{(r-k-4s)a\pi}{2^{t+1}}\right),$$

we obtain

$$T = \sum_{k=1}^{r} \sum_{a=1}^{2^t-1} \left(2\cos\frac{a\pi}{2^{t+1}}\right)^{n+r-k} \sum_{s=0}^{2^{t-1}-1} \cos\left(\frac{(r-k-4s)a\pi}{2^{t+1}}\right)$$

Formula (17.1.1) of [6] states

$$\sum_{s=0}^{N} \cos(sx+y) = \csc\frac{x}{2}\cos\left(\frac{Nx}{2}+y\right)\sin\left(\frac{(N+1)x}{2}\right). \qquad (3.12)$$

Taking $A = \frac{a\pi}{2^{t+1}}$, $N = 2^{t-1}-1$, $x = -4A$, $y = (r-k)A$ in the previous formula, we obtain

$$\begin{aligned}
&\sum_{s=0}^{2^{t-1}-1} \cos\left((r-k-4s)A\right)\\
&= \csc(-2A)\cos\left((2^{t-1}-1)(-2A)+(r-k)A\right)\sin(2^{t-1}(-2A))\\
&= \csc(2A)\sin\left(\frac{a\pi}{2}\right)\cos\left(-\frac{a\pi}{2}+(r-k+2)A\right)\\
&= \frac{1-(-1)^a}{2}\frac{\sin((r-k+2)A)}{\sin(2A)}.
\end{aligned}$$

Now, T becomes

$$\begin{aligned}
T &= \sum_{k=1}^{r}\sum_{a=1}^{2^t-1}\frac{1-(-1)^a}{2}\,(2\cos A)^{n+r-k}\cdot\frac{\sin((r-k+2)A)}{\sin(2A)}\\
&= \sum_{a=1}^{2^t-1}\frac{1-(-1)^a}{2}\frac{(2\cos A)^{n+r}}{\sin(2A)}\cdot\sum_{k=1}^{r}(2\cos A)^{-k}\sin((r-k+2)A)
\end{aligned}$$

We evaluate the inside sum using formula (14.7.1) of [6]

$$\begin{aligned}
&\sum_{k=1}^{N-1} b^k\sin(kx+y) = -\sin y + (1-2b\cos x+b^2)^{-1}\\
&\cdot[\sin y + b\sin(x-y) - b^N\sin(Nx+y) + b^{N+1}\sin((N-1)x+y)]
\end{aligned}$$

with $N=r+1$, $b=(2\cos A)^{-1}$, $x=-A$, $y=(r+2)A$. We get

$$\begin{aligned}
&\sum_{k=1}^{r}(2\cos A)^{-k}\sin((r-k+2)A)\\
&= -\sin((r+2)A) + b^{-2}(\sin((r+2)A)\\
&\qquad -b\sin((r+3)A) - b^{r+1}\sin A + b^{r+2}\sin(2A))\\
&= -\sin((r+2)A) + b^{-1}(2\cos A\sin((r+2)A)\\
&\qquad -\sin((r+3)A)) - b^{r}(2\cos A\sin A - \sin(2A))\\
&= -\sin((r+2)A) + 2\cos A\sin((r+1)A) = \sin(rA).
\end{aligned}$$

and so,

$$T = \sum_{a=1}^{2^t-1}\frac{1-(-1)^a}{2}\,(2\cos A)^{n+r-1}\,\frac{\sin(rA)}{\sin A} = \sum_{a=1,\ odd}^{2^t-1}(2\cos A)^{n+r-1}\,\frac{\sin(rA)}{\sin A}$$

Recall that our initial sum is

$$S = 2^{n+r-2} + 2^{-t}T,$$

so we need to prove $T \neq 0$. Observing that

$$a_j = \left(\cos \frac{j\pi}{2^{t+1}}\right)^{2^{t+1}+r-1} \cdot \frac{1}{\sin \frac{j\pi}{2^{t+1}}}$$

strictly decreases as j increases, $1 \leq j \leq 2^t - 1$, Lemma 3.15 shows that $T \neq 0$, thereby proving our claim. (One can prove, by a slightly more complicated method that, in fact, $T > 0$, but we did not need that.) The proof of the lemma is done. □

Lemma 3.18. *If d is odd and $2^t + 1 < d \leq 2^{t+1} - 1$ for some positive integer t, then $wt(X(d,n)) \neq 2^{n-2}$ for any n of the form $n = 2^{t+1}\ell + r$, where ℓ is even and $0 \leq r < 2^{t+1} + 2^t$.*

Proof. From equation (3.9) we have

$$wt(X(2^t+1,n)) = \sum_{k \in I(t)} \sum_{i \equiv k \pmod{2^{t+1}},\, i \leq n} C(n,i), \tag{3.13}$$

where

$$I(t) = \{k : \ k \text{ odd},\ 2^t + 1 \leq k \leq 2^{t+1} - 1\}.$$

Let $k := 2^t + 2s + 1$, where $0 \leq s \leq 2^{t-1} - 1$, and let $A_n^{2^{t+1}}(k)$ denote the inner sum in (3.13). Then Lemma 3.14 gives (with $A = \frac{j\pi}{2^{t+1}}$)

$$\begin{aligned} & A_n^{2^{t+1}}(k) \\ =& 2^{n-(t+1)} + 2^{n-t} \sum_{j=1}^{2^t-1} (\cos A)^n \cos((n-2k)A) \\ =& 2^{n-(t+1)} + 2^{n-t} \sum_{j=1}^{2^t-1} (-1)^j (\cos A)^n \cos\left((n-2-4s)A\right), \end{aligned} \tag{3.14}$$

since

$$\begin{aligned} & \cos((n-2k)A) = \cos((n-2(2^t+2s+1))A) \\ & = \cos((n-4s-2)A - 2^{t+1}A) = \cos((n-4s-2)A - j\pi) \\ & = \cos((n-4s-2)A)\cos(j\pi) + \sin((n-4s-2)A)\sin(j\pi) \\ & = (-1)^j \cos((n-4s-2)A). \end{aligned}$$

If d is odd, let $J(d) \subset I(t)$ be the subset of $I(t)$, made up of the 2^{t-2} integers k that satisfy $d \preceq k \leq 2^{t+1} - 1$ (for example, if $d = 2^t + 3$, then $J(d)$ contains every other integer in $I(t)$, starting with $2^t + 3$). Let $n = 2^{t+1}\ell + r$, $0 \leq r < 2^{t+1} + 2^t$. If

$r = 0$, Lemma 3.13 implies the result. Now, assume $1 \le r < 2^{t+1} + 2^t$. Using (3.12) we obtain (recall that $A = \frac{j\pi}{2^{t+1}}$)

$$\begin{aligned}
&\sum_{s=0}^{2^{t-1}-1} \cos\left(s(-4A) + (n-2)A\right) \\
&= \csc(-2A)\cos\left((2^{t-1}-1)(-2A) + (n-2)A\right)\sin(2^{t-1}(-2A)) \\
&= \csc(2A)\cos(-2^tA + nA)\sin(\frac{j\pi}{2}) \\
&= \csc(2A)(\cos(\frac{j\pi}{2})\cos(nA) + \sin(\frac{j\pi}{2})\sin(nA))\sin(\frac{j\pi}{2}) \qquad (3.15)\\
&= \csc(2A)\sin^2(\frac{j\pi}{2})\sin(nA) \\
&= \frac{1-(-1)^j}{2}\csc(2A)\sin((2^{t+1}\ell + r)A) \\
&= \frac{1-(-1)^j}{2}\csc(2A)(-1)^\ell\sin(rA).
\end{aligned}$$

Certainly (with $k = 2^t + 2s + 1$),

$$\begin{aligned}
wt(X(d,n)) &= \sum_{k\in J(d)} \sum_{i\equiv k \pmod{2^{t+1}},\, i\le n} C(n,i) \\
&\le \sum_{k\in I(t)} A_n^{2^{t+1}}(k) = \sum_{s=0}^{2^{t-1}-1} A_n^{2^{t+1}}(2^t + 2s + 1).
\end{aligned}$$

Then, using (3.14) and (3.15)

$$\begin{aligned}
\sum_{s=0}^{2^{t-1}-1} A_n^{2^{t+1}}(2^t + 2s + 1) &= 2^{n-2} + 2^{n-t}\sum_{s=0}^{2^{t-1}-1}\sum_{j=1}^{2^t-1}(-1)^j(\cos A)^n\cos\left((n-2-4s)A\right) \\
&= 2^{n-2} + 2^{n-t}\sum_{j=1}^{2^t-1}(-1)^j(\cos A)^n\sum_{s=0}^{2^{t-1}-1}\cos\left((n-2-4s)A\right) \\
&= 2^{n-2} + 2^{n-t}\sum_{j=1}^{2^t-1}(-1)^{\ell+j}(\cos A)^n\,\frac{1-(-1)^j}{2}\,\frac{\sin(rA)}{\sin(2A)} \\
&= 2^{n-2} + 2^{-t}(-1)^{\ell+1}\sum_{j=1,odd}^{2^t-1}(2\cos A)^{n-1}\,\frac{\sin(rA)}{\sin A} := S
\end{aligned} \qquad (3.16)$$

But the last sum is strictly positive by Lemmas 3.15 and 3.17. Therefore, if ℓ is even, $S < 2^{n-2}$, and this proves our lemma. □

The following remark summarizes our progress so far on Conjecture 1.

Remark 3.19. We see that if $n = 2^{t+1}\ell + r$, ℓ odd and $r < 2^t$, then we can write $n = 2^{t+1}\ell + r = 2^{t+1}(\ell - 1) + 2^{t+1} + r$, with $\ell - 1$ even, and $0 \le r' := 2^{t+1} + r < 2^{t+1} + 2^t$. Thus, the only cases left unchecked in the previous lemma (which gives many cases of Conjecture 1) are: $n = 2^{t+1}\ell + r$, ℓ odd, $2^t \le r < 2^{t+1}$.

4 The Case $wt(d) \ge 3$

Lemma 3.1, Corollary 3.10 and Lemma 3.17 show that Conjecture 1 holds for any $X(d,n)$ with $wt(d) = 1,2$. A key fact, given in the proof of Lemma 3.17, is a useful formula for $wt(X(d,n))$ when $wt(d) = 2$. We can find a similar formula when $wt(d) = 3$, however it becomes substantially harder to handle.

Lemma 4.1. *Let $d := 1 + 2^s + 2^t$, where $1 \le s < t$ and $t \ge 2$. Then*

$$\begin{aligned} wt(X(d,n)) = 2^{n-3} - 2^{-t} \sum_{j=1,odd}^{2^t-1} (2\cos A)^{n-1} \frac{\sin((n-2^s)A)\sin(2^sA)}{\sin A \sin(2^{s+1}A)} \\ - 2^{-s-1} \sum_{k=1,odd}^{2^s-1} (2\cos B)^{n-1} \frac{\sin(nB)}{\sin B}, \end{aligned} \tag{4.1}$$

where $A = \frac{j\pi}{2^{t+1}}$, $B = \frac{k\pi}{2^{s+1}}$.

Proof. From $d \preceq i$, we get that $i = 2^{t+1}i' + 2^t + 2^{s+1}p + 2^s + 2q + 1$, and so, $i \equiv 2^t + 2^{s+1}p + 2^s + 2q + 1 \pmod{2^{t+1}}$. Certainly the converse is also true. Using the previous observation,

$$
\begin{aligned}
wt(X(d,n)) &= \sum_{d \preceq i \leq n} C(n,i) \\
&= \sum_{p=0}^{2^{t-s-1}-1} \sum_{q=0}^{2^{s-1}-1} A_n^{2^{t+1}}(2^t + 2^{s+1}p + 2^s + 2q + 1) \\
&= \sum_{p=0}^{2^{t-s-1}-1} \sum_{q=0}^{2^{s-1}-1} (2^{n-t-1} + 2^{-t} \sum_{j=1}^{2^t-1} (2\cos A)^n \\
&\cdot \cos((n - 2^{t+1} - 2^{s+2}p - 2^{s+1} - 4q - 2)A)) \\
&= 2^{t-s-1} 2^{s-1} 2^{n-t-1} + 2^{-t} \sum_{j=1}^{2^t-1} (2\cos A)^n \qquad (4.2) \\
&\cdot \sum_{p=0}^{2^{t-s-1}-1} \sum_{q=0}^{2^{s-1}-1} \cos((n - 2^{t+1} - 2^{s+2}p - 2^{s+1} - 4q - 2)A) \\
&= 2^{n-3} + 2^{-t} \sum_{j=1}^{2^t-1} (2\cos A)^n \\
&\cdot \sum_{p=0}^{2^{t-s-1}-1} \sum_{q=0}^{2^{s-1}-1} \cos((n - 2^{t+1} - 2^{s+2}p - 2^{s+1} - 4q - 2)A)
\end{aligned}
$$

using Lemma 3.14. Further, by using formula (3.12) with $x = -4A$, $y = (n - 2^{t+1} - 2^{s+2}p - 2^{s+1} - 2)A$, $N = 2^{s-1} - 1$, the innermost sum is equal to

$$
\begin{aligned}
&\csc(x/2)\cos(Nx/2 + y)\sin((N+1)x/2) \\
&= \csc(-2A)\cos((2^{s-1} - 1)(-2A) \\
&+ (n - 2^{t+1} - 2^{s+2}p - 2^{s+1} - 2)A)\sin(2^{s-1}(-2A)) \\
&= \csc(2A)\cos((n - 2^{t+1} - 2^{s+2}p - 3 \cdot 2^s)A)\sin(2^s A),
\end{aligned}
$$

which is defined everywhere, since $j \leq 2^t - 1$. Thus,

$$
\begin{aligned}
wt(X(d,n)) &= 2^{n-3} + 2^{-t} \sum_{j=1}^{2^t-1} (2\cos A)^{n-1} \frac{\sin(2^s A)}{\sin A} \\
&\cdot \sum_{p=0}^{2^{t-s-1}-1} \cos((n - 2^{t+1} - 2^{s+2}p - 3 \cdot 2^s)A).
\end{aligned} \qquad (4.3)
$$

Let

$$U := \{j : j = 2^{t-s}k, 1 \leq k \leq 2^s - 1\}$$

We distinguish two cases:
Case 1. Assume $j \in U$. That means that

$$2^{s+2}A = 2^{s+2}\frac{j\pi}{2^{t+1}} = 2^{s+2}\frac{k2^{t-s}\pi}{2^{t+1}} = 2k\pi,$$

and using the periodicity of the cosine function, we obtain that in this case, the innermost sum is

$$2^{t-s-1}\cos((n-2^{t+1}-3\cdot 2^s)A).$$

Case 2. Assume $j \notin U$. In this case, we apply again formula (3.12) with $x = -2^{s+2}A$, $y = (n-2^{t+1}-3\cdot 2^s)A$, $N = 2^{t-s-1}-1$, the innermost sum is equal to

$$\begin{aligned}
&\csc(-2^{s+1}A)\cos((2^{t-s-1}-1)(-2^{s+1}A)\\
&+(n-2^{t+1}-3\cdot 2^s)A)\sin(2^{t-s-1}(-2^{s+1}A))\\
&=\csc(2^{s+1}A)\cos(-2^tA+(n-2^{t+1}-2^s)A)\sin(2^tA)\\
&=\csc(2^{s+1}A)\cos((n-2^s)A-3j\pi/2)\sin(j\pi/2)\\
&=\csc(2^{s+1}A)\cos((n-2^s)A+j\pi/2)\sin(j\pi/2)
\end{aligned}$$

Thus, from equation (4.3), we obtain (note that $A = B$, if $j = 2^{t-s}k$; also, $2^{t+1}A = j\pi$, $2^sB = k\pi/2$)

$$\begin{aligned}
wt(X(d,n)) &= 2^{n-3} + 2^{-t}\sum_{j=1,j\notin U}^{2^t-1}(2\cos A)^{n-1}\frac{\cos((n-2^s)A+j\pi/2)\sin(j\pi/2)\sin(2^sA)}{\sin A\sin(2^{s+1}A)}\\
&+ 2^{-t}\sum_{j=1,j\in U}^{2^t-1}(2\cos A)^{n-1}\frac{\sin(2^sA)}{\sin A}2^{t-s-1}\cos((n-3\cdot 2^s)A-j\pi)\\
&= 2^{n-3} + 2^{-t}\sum_{j=1,j\notin U}^{2^t-1}(2\cos A)^{n-1}\frac{\cos((n-2^s)A+j\pi/2)\sin(j\pi/2)\sin(2^sA)}{\sin A\sin(2^{s+1}A)}\\
&+ 2^{-s-1}\sum_{k=1}^{2^s-1}(2\cos B)^{n-1}\frac{\sin(k\pi/2)}{\sin B}\cos((n-3\cdot 2^s)B-2^{t-s}k\pi)
\end{aligned}$$

$$\begin{aligned}
&= 2^{n-3} + 2^{-t}\sum_{j=1,j\notin U}^{2^t-1}(2\cos A)^{n-1}\frac{\cos((n-2^s)A+j\pi/2)\sin(j\pi/2)\sin(2^sA)}{\sin A\sin(2^{s+1}A)}\\
&+ 2^{-s-1}\sum_{k=1}^{2^s-1}(2\cos B)^{n-1}\frac{\sin(k\pi/2)}{\sin B}\cos(nB+k\pi/2).
\end{aligned} \tag{4.4}$$

(The last equality follows from the periodicity of cos, and also from $\cos((n-3\cdot 2^s)B) = \cos(nB-3k\pi/2) = \cos(nB+k\pi/2)$.) Further, if $j \notin U$, then $\sin(2^{s+1}A)$ is well defined, however $\sin(j\pi/2) = 0$, if j is even. Thus, the terms in the first sum of the last equation of (4.4) are zero, unless j is odd. Then, if j is odd, we get

$$\begin{aligned}&\cos((n-2^s)A + j\pi/2)\sin(j\pi/2)\\ &= (\cos((n-2^s)A)\cos(j\pi/2) - \sin((n-2^s)A)\sin(j\pi/2))\sin(j\pi/2)\\ &= -\sin((n-2^s)A).\end{aligned}$$

Therefore,

$$\begin{aligned}wt(X(d,n)) = 2^{n-3} - 2^{-t}\sum_{j=1,odd}^{2^t-1}(2\cos A)^{n-1}\cdot\frac{\sin((n-2^s)A)\sin(2^sA)}{\sin A\sin(2^{s+1}A)}\\ + 2^{-s-1}\sum_{k=1}^{2^s-1}(2\cos B)^{n-1}\frac{\sin(k\pi/2)}{\sin B}\cos(nB + k\pi/2)\end{aligned}$$

or better, yet,

$$\begin{aligned}wt(X(d,n)) = 2^{n-3} - 2^{-t}\sum_{j=1,odd}^{2^t-1}(2\cos A)^{n-1}\frac{\sin((n-2^s)A)\sin(2^sA)}{\sin A\sin(2^{s+1}A)}\\ - 2^{-s-1}\sum_{k=1,odd}^{2^s-1}(2\cos B)^{n-1}\frac{\sin(nB)}{\sin B}\end{aligned}$$

□

In order to prove Conjecture 1, by Lemma 3.1 and Corollary 3.10 it would suffice to show that for $n \geq 2(d-1)$ (we can assume this because of Theorem 2.2) we have

$$wt(X(d,n)) \neq 2^{n-2} \tag{4.5}$$

for all pairs d, n except $d = 2^t + 1, n = 2^{t+1}\ell$, where t and ℓ are any positive integers.

Lemma 3.17 proves (4.5) when $wt(d) = 2$ (if d is odd with $wt(d) = 2$, then $d = 2^t + 1$; further, if $n \geq 2(d-1)$, then $n \geq 2^{t+1}$ and if 2^{t+1} does not divide n, then $n = 2^{t+1}\ell + r$ with $r \not\equiv 0 \pmod{2^{t+1}}$ and so Lemma 3.17 applies; if 2^{t+1} does divide n, then we already know from Theorem 1, which summarizes the results of [5] that $X(d,n)$ is balanced).

We attempted to prove (4.5) when $wt(d) = 3$ by using Lemma 4.1, but the sums in (4.1) were too complicated to allow us to cover all of the cases. Certainly (4.1) shows that for fixed d, (4.5) holds for all sufficiently large n, because the factors $(\cos A)^{n-1}$ and $(\cos B)^{n-1}$ tend to 0 as $n \to \infty$, which implies $wt(X(d,n)) - 2^{n-2} < 0$ for all large n. Our computations suggest that this inequality will always hold if $wt(d)$ is large enough. In fact, we conjecture that the following stronger form of Conjecture 1 is true when $wt(d) \geq 6$:

Conjecture 2. If $n \geq 2(d-1)$, d is fixed and $wt(d) \geq 6$, then $wt(X(d,n)) < 2^{n-2}$.

Acknowledgments. The authors would like to thank Prof. Jingbo Xia for the proof of Lemma 3.15, which simplified their original argument.

References

[1] P. Stănică, *Chromos, Boolean Functions and Avalanche Characteristics*, Ph.D. thesis, State University of New York at Buffalo, 1998.

[2] J.O. Brüer, *On pseudorandom sequences as crypto generators*, pp. 157–161, Proc. 1984 Int. Zürich Seminar on Digital Communications, Zürich, Switzerland, 1984.

[3] A. Canteaut and M. Videau, *Symmetric Boolean Functions*, IEEE Trans. on Information Theory 51 (2005), pp. 2791–2811.

[4] C. Carlet, *On cryptographic propagation criteria for Boolean functions*, Inform. and Comput. 151 (1999), pp. 32–56.

[5] T.W. Cusick, Yuan Li, and P. Stănică, *Balanced Symmetric Functions over $GF(p)$*, IEEE Trans. on Information Theory 54 (2008), pp. 1304–1307.

[6] E.R. Hansen, *A Table of Series and Products*. Prentice-Hall, Englewood Cliffs, NJ, 1975.

[7] V.E. Hoggatt Jr. and G.L. Alexanderson, *Sums of partition sets in generalized Pascal triangles I*, Fibonacci Quarterly 14 (1976), pp. 117–125.

[8] T. Lengyel, *On the order of lacunary sums of binomial coefficients*, Integers 3 (2003). 10 pp.

[9] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North Holland, 1978.

Received xxx; revised xxx

Author information

Thomas W. Cusick, SUNY, Department of Mathematics
244 Mathematics Building
Buffalo, NY 14260, U.S.A..
Email: cusick@buffalo.edu

Yuan Li, Department of Mathematics
Winston-Salem State University
Winston-Salem, NC 27110, U.S.A..
Email: yuanli7983@gmail.com

Pantelimon Stănică, Applied Mathematics Department
Naval Postgraduate School
Monterey, CA 93943, U.S.A..
Email: pstanica@nps.edu